Seguridad Informatica y Analisis Forence

Alejandro Manuel Ruanova Lopez

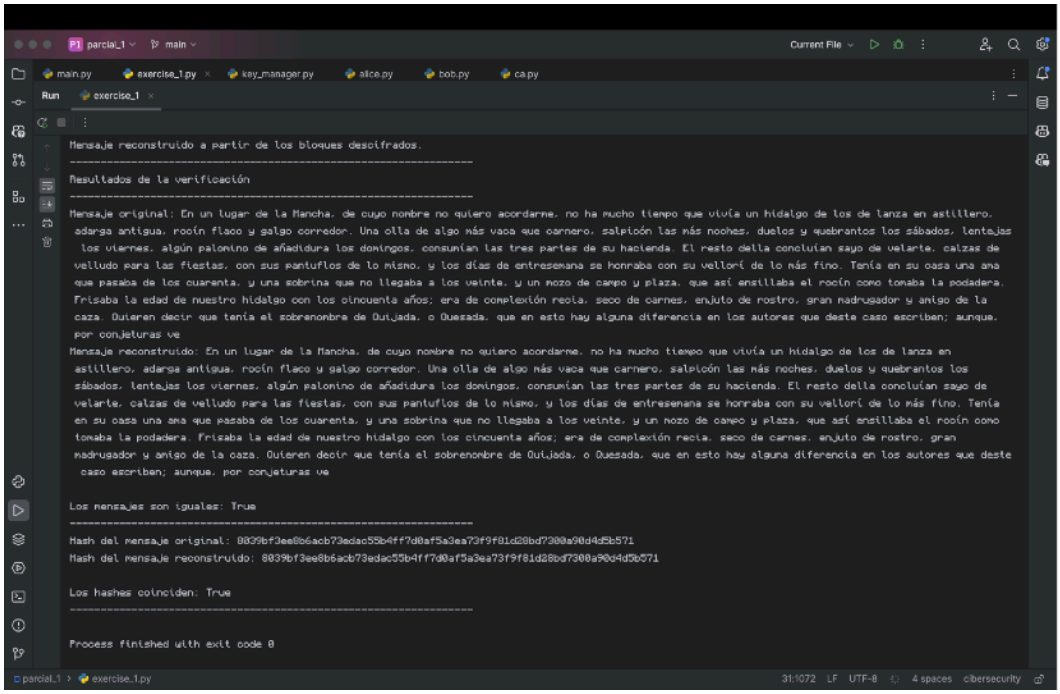
01/03/2024

00431278

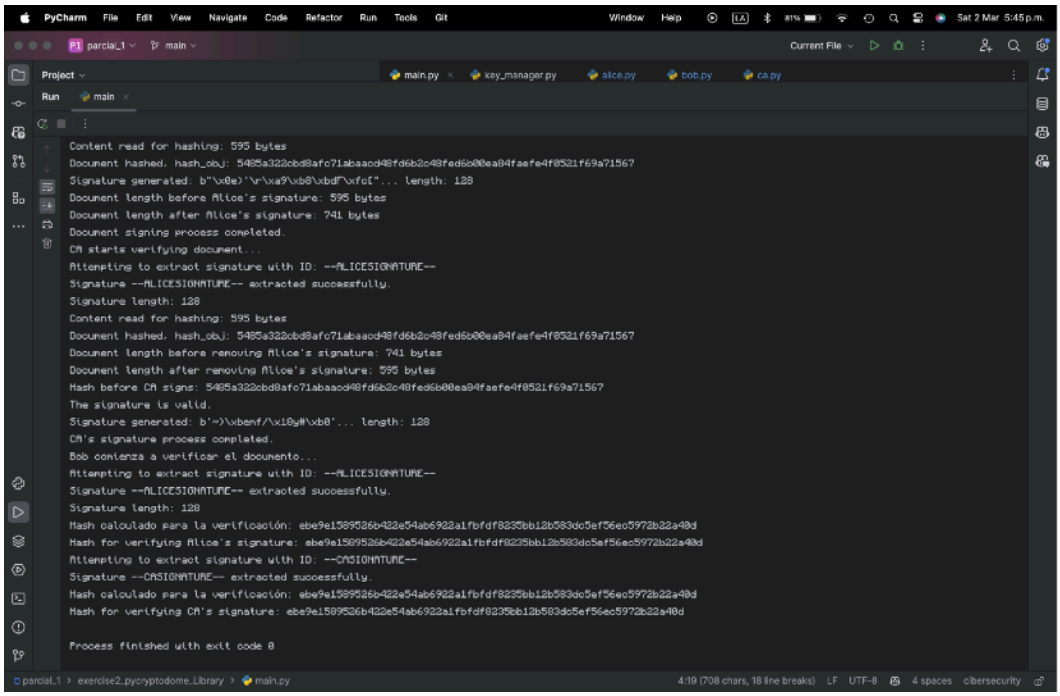
Documento de Evidencia

Evidencia capturas

Ejercicio 1:



Ejercicio 2:



Preguntas:

Importancia del método RSA en el contexto del protocolo HTTPS: El método RSA (Rivest-Shamir-Adleman) es fundamental para el protocolo HTTPS, ya que proporciona una forma segura de cifrado de datos. HTTPS, que significa HyperText Transfer Protocol Secure, es la versión segura del HTTP y es utilizado para la transmisión segura de datos en Internet. RSA juega un papel crucial al permitir el intercambio seguro de claves entre el navegador del usuario y el servidor web, lo que es esencial para establecer una sesión segura. Mediante el uso de un sistema de cifrado asimétrico, RSA facilita que las partes intercambien claves de cifrado de manera segura sin necesidad de un canal seguro preestablecido. Esto asegura que la información transmitida, como datos personales y financieros, esté protegida contra interceptaciones y accesos no autorizados.

Capa 7 del modelo OSI y los principales ataques a dicha capa: La capa 7 del modelo OSI, también conocida como la capa de aplicación, es la capa más alta y se encarga de facilitar las interacciones entre las aplicaciones de los usuarios finales y la red. En esta capa, se realizan funciones como la representación de datos, el cifrado y el manejo de sesiones. Los principales ataques dirigidos a esta capa incluyen:

- Inyección de SQL: Ataques que explotan vulnerabilidades de las aplicaciones web para ejecutar comandos SQL no autorizados en una base de datos.
- Cross-Site Scripting (XSS): Ataques que insertan código malicioso en páginas web vistas por otros usuarios para robar información como cookies o datos de sesión.

- Cross-Site Request Forgery (CSRF): Ataques que engañan a un navegador web para realizar acciones no deseadas en un sitio web en el que el usuario ha iniciado sesión.
- Ataques de Denegación de Servicio (DoS y DDoS): Aunque pueden afectar a varias capas, en la capa 7 se pueden realizar ataques específicos que sobrecargan las aplicaciones web, haciéndolas inaccesibles.

Importancia del algoritmo RSA en mis propias palabras: El algoritmo RSA es como tener un candado y una llave en el mundo digital. Imagina que quieres enviar un mensaje secreto en una caja fuerte a alguien. Con RSA, puedes cerrar esta caja fuerte con un candado que solo se puede abrir con una llave única. Solo el destinatario de tu mensaje tiene la llave correcta (clave privada), mientras que cualquier persona puede cerrar la caja (usando la clave pública). Esto hace que el RSA sea increíblemente valioso para proteger nuestra información en línea, asegurando que solo las personas correctas puedan acceder a los datos sensibles que enviamos a través de Internet.

Uso del cifrado asimétrico usando RSA en la vida real: El cifrado asimétrico RSA se puede usar en una variedad de aplicaciones prácticas en la vida real, tales como:

- Comunicaciones seguras por email: Cifrar mensajes de correo electrónico para garantizar que solo el destinatario pueda leerlos.
- Autenticación: Verificar la identidad de los usuarios y los dispositivos en las redes para prevenir el acceso no autorizado.
- Firma digital: Asegurar la integridad y la autenticidad de los documentos digitales, haciendo que el proceso de firma sea verificable y no repudiable.
- Transacciones seguras en línea: Proteger la información de las tarjetas de crédito y otras transacciones financieras en Internet.

Importancia de la ciberseguridad y cómo protegernos: La ciberseguridad es esencial en nuestro entorno actual debido a la creciente dependencia de la tecnología y la Internet para realizar actividades cotidianas, como comunicarse, comprar y trabajar. Proteger nuestra información personal y la infraestructura crítica de los ciberataques es crucial para mantener nuestra privacidad, seguridad económica y seguridad nacional. Para protegernos, debemos adoptar prácticas de seguridad sólidas, como el uso de contraseñas fuertes y únicas, habilitar la autenticación de dos factores, mantener actualizado el software, ser cautelosos con los enlaces y archivos adjuntos en correos electrónicos, y educarnos sobre las últimas amenazas de seguridad para poder reconocer y evitar ataques cibernéticos.